REMARKS

In the Office Action the Examiner noted that claims 1-18 are pending in the application, and the Examiner rejected all claims. By this Amendment, claims 3-5, 7, 9-10, and 12-14 have been cancelled without prejudice or disclaimer, and claims 1-2, 6, 11, and 15-18 have been amended. Features incorporated in the amendments of the amended claims were recited in at least original claims 3-4, which are now cancelled, and therefore no new matter has been presented. Thus, claims 1-2, 6, 8, 11, and 15-18 remain pending in the application. The Examiner's rejections are traversed below, and reconsideration of all rejected claims is respectfully requested.

Examiner's Response To Arguments

In item 2 on pages 2-3 of the Office Action the Examiner stated that the Applicant's arguments filed on April 19, 2006 had been fully considered, and listed reasons for which the arguments were not found to be persuasive. The arguments referred to U.S. Patent No. 5,991,881, issued to Conklin et al. (hereinafter referred to as "Conklin"), which the Examiner relied upon for the rejections of the previous and current Office Actions. The Applicant offers the following rebuttals to several statements made in the Examiner's reasons for the arguments not being persuasive.

The Examiner stated that the Applicant's argument that Conklin does not disclose "detection of a computer virus in information transmitted from the terminal apparatus to the central apparatus by the installed anti-virus software" is not persuasive because Conklin discloses a network surveillance system situated on a network to monitor and log all communications between terminal apparatuses. The Examiner concluded that traffic between a central apparatus and a terminal apparatus is monitored and recorded because all the packets are passed through the network surveillance system.

However, the Applicant respectfully submits that, contrary to the Examiner's statement, not all the traffic between a central apparatus and a terminal apparatus is monitored and recorded. It is clear from Figure 6 of Conklin, as well as Lines 23-24 of Column 5, that if there is no indication of an actual or potential intrusion, then the packet is discarded rather than recorded. The Examiner relied upon Lines 30-34 of Column 4 of Conklin to support the allegation that the recorded logs are examined for possible intrusion patterns. However, it is apparent from the disclosure of Conklin that the intrusion detection process discussed in Lines 30-34 of Column 4 is performed before any packet is recorded in a log.

Further, the claim clearly recites that the installed anti-virus software detects the computer virus information, and that the anti-virus software is installed on the central apparatus. The Examiner acknowledged that the network surveillance system is not the recited central apparatus in the following statements:

> All the packets transmitted between terminal apparatuses are also passed through the network surveillance system (column 3 lines 51-56). Therefore it is asserted that traffic between a central apparatus and a terminal apparatus is monitored and recorded.

Therefore, it is clear that Conklin does not disclose or suggest the recited feature of "detection of a computer virus in information transmitted from the terminal apparatus to the central apparatus by the installed anti-virus software." In other words, while the network surveillance system may detect an intruder in packets transmitted between a terminal apparatus and the central apparatus, it is clear that no detection of a computer virus is performed by anti-virus software installed on the central apparatus.

It is further noted that although the Examiner acknowledged that the network surveillance system is not the recited central apparatus in the statements discussed above, the Examiner also went on to state:

> Therefore, the network surveillance system (central apparatus) detects a virus in information transmitted between the terminal apparatus and the central apparatus.

The Applicant respectfully submits that it is improper to characterize the network surveillance system as the central apparatus after earlier stating that the network surveillance system monitors traffic between a central apparatus and a terminal apparatus.

Also, the Examiner stated that the Applicant's argument that Conklin does not disclose "storing a communication history of the terminal apparatus" is not persuasive because Conklin "writes a log of the network traffic (column 4 lines 16-29), which is then analyzed for possible intrusion patterns (column 4 lines 30-39)." However, as already discussed in this response, the network traffic is not logged for the intrusion detection process cited by the Examiner. Rather, the packets that are reported from the intrusion detection process are then logged, and the other packets are discarded. "The Evidence Logging function responds to the Reportable Activity from the Intrusion Detection function and that Evidence Logging Function responsively writes a log of the associated network traffic and provides a responsive indication to the Incident

Analyzer/Reporter shown in FIG. 6e and its Event Log Analyzing Function" (Column 4, Lines 16-22). In other words, only the packets having reportable activity are logged, and the reportable activity analysis and discarding of other packets occurs before being logged.

Finally, the Examiner stated that the Applicant's argument that Conklin does not disclose "specifying the time of infection" is not persuasive because Conklin discloses a continuous monitoring, recording, and analyzing process, wherein traffic is recorded and analyzed, and if an intrusion is found, a data structure is formed with a date-time stamp indicating the time of detection. The Examiner went on to allege that this process is analogous to the time of infection, and therefore Conklin discloses specifying a time of infection.

The Applicant respectfully submits that no one skilled in the art would reasonably characterize the above-described "time of detection" as a "time of infection." The "time of detection" recorded in Conklin is simply that – the time at which an intruder was detected. However, this is in no way indicative of when the terminal apparatus was infected with a computer virus infection. Rather, the time of detection merely indicates that an infection has occurred before that point in time. This is not tantamount to "transmitting the infection information including the specified time of infection". Also, as already discussed, Conklin does not disclose continuous recording and analysis, as again alleged by the Examiner. Rather, a log is only recorded if the intrusion detection process detects any reportable activity.

Therefore, the Applicant respectfully submits that the previously filed traversals of the Examiner's rejections base on Conklin have not been overcome. Nevertheless, amendments have been made to several of the claims, as explained below, and the Applicant respectfully submits that the application is in condition for allowance.

Claim Rejections Under 35 USC §102

In item 3 on pages 4-18 the Examiner rejected claims 1-18 under 35 U.S.C. §102(b) as being anticipated by Conklin. By this Amendment, claims 3-5, 7, 9-10, and 12-14 have been cancelled without prejudice or disclaimer. The Applicant respectfully traverses the Examiner's rejections of the remaining claims.

Claim 1 of the present application, as amended, recites "specifying a time of infection of the terminal apparatus based on the stored communication history, the registered time of find-out, and a time of installation of the anti-virus software, in response to detection, by the installed anti-virus software, of the computer virus in information transmitted from the terminal apparatus to the central apparatus." The Applicant respectfully submits that Conklin does not disclose or suggest at least this feature of claim 1.

As discussed in the previous section of this Response, Conklin does not disclose specifying the time of infection of the terminal apparatus at all. Conklin merely discloses a network surveillance system detecting an intruder to a computer system, and upon detection of the intruder recording a date and time stamp of the detection time (Column 5, Lines 23-32). Otherwise all transmitted packets are discarded by the network surveillance system. Therefore, Conklin merely discloses noting the time that an intruder is detected.

This is in direct contrast to specifying a time of infection of the terminal apparatus based on the stored communication history, the registered time of find-out, and a time of installation of the anti-virus software, as is recited in claim 1 of the present application. Because there is a stored communication history, the method recited in claim 1 allows the central apparatus to compare the time of the communication containing the infection to the time of a previous communication stored in the communication history, and therefore the central apparatus is able to transmit the time of infection to the terminal apparatus. Conklin cannot perform this operation because there is no stored communication history of the terminal apparatus. Rather, Conklin can merely report that an infection has been detected.

Also, as discussed in the previous section of this Response, the time of infection is not analogous to the time of detection. The Examiner's statement to the contrary would apparently contain the logical implication that infection and detection happens simultaneously, which would not be accepted by any person skilled in the art. For instance, if a terminal apparatus were to be infected by a virus contained on a disc read by the terminal apparatus, and that virus operated to later send an email communication to replicate the virus elsewhere, it is obvious that the detection time of that infected email would not be tantamount to the time in which the terminal apparatus was actually infected. Instead, it would merely indicate that the terminal apparatus was infected at some time before the detection, which is an obvious conclusion without any report generated by Conklin. Again, because Conklin stores no history of communications before detecting the intruder, there is no way for Conklin to determine the time of infection.

Further, claim 1 of the present application recites "specifying a route of infection of the computer virus based on the stored communication history and the time of installation of the anti-virus software." Therefore, in one embodiment enabled by the recitation of claim 1, the time of infection and the route of infection are able to be determined because of the stored communication history, the registered time of find-out, and the time of installation of the anti-virus software. The Applicant respectfully submits that Conklin also does not disclose, suggest, or contemplate this feature of claim 1.

The Examiner stated that Conklin discloses, in Lines 23-32 of Column 5, registering the time of find-out and specifying the route of infection of the computer virus based on the stored communication history and the time of installation, wherein the source and destination IP addresses are recorded. However, the Applicant respectfully submits that Conklin merely discloses recording the time when communication data was sent/received, an address of the addressee included in the communication data, and an address of the sender. Accordingly, in the event wherein an intruder directly sends communication data, it may be possible to specify the infection route by the address information thus recorded in Conklin. However, in one embodiment enabled by claim 1 of the present application, the time when an apparatus is infected by a computer virus, as well as the route of infection, can be determined based on the time of installation of anti-virus software, operation history, communication history with a central apparatus, and the date and time of detection of the virus. The Applicant respectfully submits that these features are not disclosed, suggested, or contemplated by Conklin.

To wit, claim 1 of the present application recites "registering a time of find-out, which is the time when the computer virus was found out. The time of infection is specified based on the stored communication history, the registered time of find-out, and the time of installation of the anti-virus software, which is the time when the anti-virus software was installed. Conklin does not disclose or even contemplate registering the time of find-out, but the Examiner, by citing Lines 23-32 of Column 5 of Conklin, apparently characterizes the logging of the time of detection as both the time of find-out and the time of infection, although the time of infection is based upon, in part, the time of find-out. The Applicant respectfully submits that this is not a reasonable characterization, and in fact is not even possible. In essence, the Examiner stated that the determination of the time of infection is based on the time of infection, which the Applicant respectfully submits is not a logically reasonable assertion.

Therefore, Conklin does not disclose or suggest at least the features of claim 1 discussed above. Accordingly, Conklin does not disclose every element of the Applicant's claim 1. In order for a reference to anticipate a claim, the reference must teach each and every element of the claim (MPEP §2131). Therefore, since Conklin does not disclose the features recited in independent claim 1, as stated above, it is respectfully submitted that claim 1 patentably distinguishes over Conklin, and withdrawal of the §102(b) rejection is earnestly and respectfully solicited.

Claim 2 of the present application recites similar features to those discussed above in regard to claim 1, and which are not disclosed or suggested by Conklin. Therefore, it is respectfully submitted that claim 2 also patentably distinguishes over Conklin.

Claims 6 and 8 depend from claim 2 and include all of the features of that claim plus additional features which are not disclosed or suggested by Conklin. Therefore, it is respectfully submitted that claims 6 and 8 also patentably distinguish over Conklin.

Independent claims 11 and 15-18 all recite similar features to those discussed above in regard to claim 1, and which are not disclosed or suggested by Conklin. Therefore, it is respectfully submitted that claims 11 and 15-18 also patentably distinguish over Conklin.

Summary

In accordance with the foregoing, claims 3-5, 7, 9-10, and 12-14 have been cancelled without prejudice or disclaimer, and claims 1-2, 6, 11, and 15-18 have been amended. No new matter has been presented. Thus, claims 1-2, 6, 8, 11, and 15-18 remain pending in the application

There being no further outstanding objections or rejections, it is respectfully submitted that the application is in condition for allowance. An early action to that effect is courteously solicited.

Finally, if there are any formal matters remaining after this response, the Examiner is requested to telephone the undersigned to attend to these matters.

If there are any additional fees associated with filing of this Amendment, please charge the same to our Deposit Account No. 19-3935.

Respectfully submitted,

STAAS & HALSEY LLP

Date: 10/04/06

By: Thomas L. Jones
Thomas L. Jones
Registration No. 53,908

1201 New York Avenue, NW, 7th Floor
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501